Rick Klingbeil, OSB #933326
RICK KLINGBEIL, PC
520 SW Sixth, Suite 950
Portland, OR 97204
Ph: (503) 473-8565
rick@klingbeil-law.com

Brady Mertz, OSB #970814, WSB #32558
2285 Liberty St NE
Salem OR 97301
Ph: (503) 385-0121
brady@bradymertz.com

Brooks Cooper, OSB #941772, WSB #32460
520 SW 6th Ave., Ste. 914
Portland OR 97204
Ph: (971) 645-4433
brooks@bcooper-law.com

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

PORTLAND DIVISION

VICKI VAN VALIN, on behalf of herself and all others similarly situated within the state of Oregon; NEIL MERTZ on behalf of himself and all other similarly situated within the state of Washington; Plaintiffs, v. **GOOGLE, INC., a Delaware corporation;** Defendant.	No. CV 10-557 ST **DECLARATION OF RICK KLINGBEIL IN SUPPORT OF MOTION FOR TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION - FRCP 65(b)**

I, Rick Klingbeil, declare as follows:

1. I am a competent adult resident of the state of Oregon, and one of plaintiffs' attorneys. I make this declaration based on personal knowledge, and in support of plaintiffs' Motion

for Temporary Restraining Order and Preliminary Injunction, filed concurrently.

2. The attached pages 1 and 2 of Exhibit "A" are true and correct copies of documents (with yellow highlighting added by counsel) that I obtained from a website that, on information and belief, is hosted by Google, Inc. the defendant in this case. The URL (address) where these pages were located is: http://googleblog.blogspot.com/search?q=wifi+data+collection.

The attached pages 3 and 4 of Exhibit "A" are true and correct copies of documents (with yellow highlighting added by counsel) that I obtained from a website that, on information and belief, is hosted by Google, Inc. The URL (address) where these pages were located is: http://googlepolicyeurope.blogspot.com/2010/04/data-collected-by-google-cars.html.

The attached pages 5 through 10 of Exhibit "A" are true and correct excerpts of pages published by the following news sources, and obtained from websites maintained or controlled by each: The Register, The Guardian, and eWEEK. The yellow highlighting was added by counsel.

3. The attached Exhibit "B" is a true and correct copy of a letter and exhibit that on May 14, 2010 I mailed by first class mail to the published home office address for Google, Inc, at:

Google, Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043,

and sent on that day to Google, Inc. at its published facsimile number: 1-650-253-0001.

4. The attached Exhibit "C" is a true and correct copy of the confirmation sheet produced by the facsimile system used by my office.

I declare under penalty of perjury, and pursuant to the provisions of 28 U.S.C. § 1746 that the foregoing is true and correct.

Signed at Portland, Oregon on May 18, 2010.

Rick Klingbeil

The Official Google Blog

Insights from Googlers into our products, technology, and the Google culture.

Showing newest posts with label **security**. Show older posts

WiFi data collection: An update

5/14/2010 01:44:00 PM

Update May 17, 2010:

On Friday May 14 the Irish Data Protection Authority asked us to delete the payload data we collected in error in Ireland. We can confirm that all data identified as being from Ireland was deleted over the weekend in the presence of an independent third party. We are reaching out to Data Protection Authorities in the other relevant countries about how to dispose of the remaining data as quickly as possible.

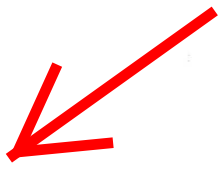
You can read the letter from the independent third party, confirming deletion, here.

[original post]
Nine days ago the data protection authority (DPA) in Hamburg, Germany asked to audit the WiFi data that our Street View cars collect for use in location-based products like Google Maps for mobile, which enables people to find local restaurants or get directions. His request prompted us to re-examine everything we have been collecting, and during our review we discovered that a statement made in a blog post on April 27 was incorrect.

In that blog post, and in a technical note sent to data protection authorities the same day, we said that while Google did collect publicly broadcast SSID information (the WiFi network name) and MAC addresses (the unique number given to a device like a WiFi router) using Street View cars, we did not collect payload data (information sent over the network). But it's now clear that we have been mistakenly collecting samples of payload data from open (i.e. non-password-protected) WiFi networks, even though we never used that data in any Google products.

However, we will typically have collected only fragments of payload data because: our cars are on the move; someone would need to be using the network as a car passed by; and our in-car WiFi equipment automatically changes channels roughly five times a second. In addition, we did not collect information traveling over secure, password-protected WiFi networks.

So how did this happen? Quite simply, it was a mistake. In 2006 an engineer working on an experimental WiFi project wrote a piece of code that sampled all categories of publicly broadcast WiFi data. A year later, when our mobile team started a project to collect basic WiFi network data like SSID information and MAC addresses using Google's Street View cars, they included that code in their software—although the project leaders did not want, and had no intention of using, payload data.



As soon as we became aware of this problem, we grounded our Street View cars and segregated the data on our network, which we then disconnected to make it inaccessible. We want to delete this data as soon as possible, and are currently reaching out to regulators in the relevant countries about how to quickly dispose of it.

Maintaining people's trust is crucial to everything we do, and in this case we fell short. So we will be:

- Asking a third party to review the software at issue, how it worked and what data it gathered, as well as to confirm that we deleted the data appropriately; and
- Internally reviewing our procedures to ensure that our controls are sufficiently robust to address these kinds of problems in the future.

In addition, given the concerns raised, we have decided that it's best to stop our Street View cars collecting WiFi network data entirely.

This incident highlights just how publicly accessible open, non-password-protected WiFi networks are today. Earlier this year, we encrypted Gmail for all our users, and next week we will start offering an encrypted version of Google Search. For other services users can check that pages are encrypted by looking to see whether the URL begins with "https", rather than just "http"; browsers will generally show a lock icon when the connection is secure. For more information about how to password-protect your network, read this.

The engineering team at Google works hard to earn your trust—and we are acutely aware that we failed badly here. We are profoundly sorry for this error and are determined to learn all the lessons we can from our mistake.

Posted by Alan Eustace, Senior VP, Engineering & Research

Permalink Links to this post

Share:

Labels: privacy, security

A new approach to China

1/12/2010 03:00:00 PM

Like many other well-known organizations, we face cyber attacks of varying degrees on a regular basis. In mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google. However, it soon became clear that what at first appeared to be solely a security incident--albeit a significant one--was something quite different.

First, this attack was not just on Google. As part of our investigation we have discovered that at least twenty other large companies from a wide range of businesses--including the Internet, finance, technology, media and chemical sectors--have been similarly targeted. We are currently in the process of notifying those companies, and we are also working with the relevant U.S. authorities.

Second, we have evidence to suggest that a primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists. Based on our investigation to date we believe their attack did not achieve that objective. Only two Gmail accounts appear to have been accessed, and that activity was limited to account information (such as the date the account was created) and subject line, rather than the content of emails themselves.

Third, as part of this investigation but independent of the attack on Google, we have discovered that the accounts of dozens of U.S.-, China- and Europe-based Gmail users who are advocates of human rights in China appear to have been routinely accessed by third parties. These accounts have not been accessed through any security breach at Google, but most likely via phishing scams or malware placed on the users' computers.

We have already used information gained from this attack to make infrastructure and architectural improvements that enhance security for Google and for our users. In terms of individual users, we would advise people to deploy reputable anti-virus and anti-spyware programs on their computers, to install patches for their operating systems and to update their web browsers. Always be cautious when clicking on links appearing in instant messages and emails, or when asked to share personal information like passwords online. You can read more here about our cyber-security recommendations. People wanting to learn more about these

European Public Policy Blog

Google's views on government, policy and politics in Europe

Data collected by Google cars

Tuesday, April 27, 2010 | 1:01 PM

Labels: Germany, privacy, Street View

[Editor's note, 5/14/10: This post contains incorrect information about our WiFi data collection (see * below). We have posted a clarification and update about our process on the Official Google Blog.]

Over the weekend, there was a lot of talk about exactly what information Google Street View cars collect as they drive our streets. While we have talked about the collection of WiFi data a number of times before--and there have been stories published in the press--we thought a refresher FAQ pulling everything together in one place would be useful. This blog also addresses concerns raised by data protection authorities in Germany.

What information are your cars collecting?
We collect the following information--photos, local WiFi network data and 3-D building imagery. This information enables us to build new services, and improve existing ones. Many other companies have been collecting data just like this for as long as, if not longer, than Google.

- **Photos**: so that we can build Street View, our 360 degree street level maps. Photos like these are also being taken by TeleAtlas and NavTeq for Bing maps. In addition, we use this imagery to improve the quality of our maps, for example by using shop, street and traffic signs to refine our local business listings and travel directions;
- **WiFi network information**: which we use to improve location-based services like search and maps. Organizations like the German Fraunhofer Institute and Skyhook already collect this information globally;
- **and 3-D building imagery**: we collect 3D geometry data with low power lasers (similar to those used in retail scanners) which help us improve our maps. NavTeq also collects this information in partnership with Bing. As does TeleAtlas.

What do you mean when you talk about WiFi network information?
WiFi networks broadcast information that identifies the network and how that network operates. That includes SSID data (i.e. the network name) and MAC address (a unique number given to a device like a WiFi router).

Networks also send information to other computers that are using the network, called payload data, but Google does not collect or store payload data.*

But doesn't this information identify people?
MAC addresses are a simple hardware ID assigned by the manufacturer. And SSIDs are often just the name of the router manufacturer or ISP with numbers and letters added, though some people do also personalize them.

However, we do not collect any information about householders, we cannot identify an individual from the location data Google collects via its Street View cars.

Is it, as the German DPA states, illegal to collect WiFi network information?
We do not believe it is illegal--this is all publicly broadcast information which is accessible to anyone with a WiFi-enabled device. Companies like Skyhook have been collecting this data cross Europe for longer than Google, as well as organizations like the German Fraunhofer Institute.

Why did you not tell the DPAs that you were collecting WiFi network information?
Given it was unrelated to Street View, that it is accessible to any WiFi-enabled device and that other companies already collect it, we did not think it was necessary. However, it's clear with

Search our Blog

Site Feed

Google™

BY FEEDBURNER

Archive

2010 (31)

Recent Posts

WiFi data collection: An update
A Polish Internet Revolution
TechTalk: Search Quality
German Supreme Court rules that Image Search does not infringe copyright
Disrupting knowledge workers - e.g. lawyers

Labels

Academics (3)
Advertising (3)
Brussels Tech Talk (4)
Child Safety (2)
Cloud computing (5)
Competition (6)
Consumers (6)
Controversial Content (1)
copyright (6)
Energy + Environment (2)
European Parliament (2)
European Union (41)
France (3)
Free Expression (6)
Germany (3)
Innovation (24)
Internet Governance (2)
IP (5)
Italy (4)
Poland (2)
Politics (1)
Power of Data (5)
privacy (21)
Publishing (13)
Russia (1)
Single Market (4)

Why did you not tell the DPAs that you were collecting WiFi network information?
Given it was unrelated to Street View, that it is accessible to any WiFi-enabled device and that other companies already collect it, we did not think it was necessary. However, it's clear with hindsight that greater transparency would have been better.

Why is Google collecting this data?
The data which we collect is used to improve Google's location based services, as well as services provided by the Google Geo Location API. For example, users of Google Maps for Mobile can turn on "My Location" to identify their approximate location based on cell towers and WiFi access points which are visible to their device. Similarly, users of sites like Twitter can use location based services to add a geo location to give greater context to their messages.

Can this data be used by third parties?
Yes--but the only data which Google discloses to third parties through our Geo Location API is a triangulated geo code, which is an approximate location of the user's device derived from all location data known about that point. At no point does Google publicly disclose MAC addresses from its database (in contrast with some other providers in Germany and elsewhere).

Do you publish this information?
No.

But wouldn't GPS enable you to do to all this without collecting the additional data?
Yes--but it can be much slower or not available (e.g. when there is no view of the sky; when blocked by tall buildings). Plus many devices don't have GPS enabled. GPS is also expensive in terms of battery consumption, so another reason to use WiFi location versus GPS is to conserve energy.

How does this location database work?
Google location based services using WiFi access point data work as follows:

- The user's device sends a request to the Google location server with a list of MAC addresses which are currently visible to the device;
- The location server compares the MAC addresses seen by the user's device with its list of known MAC addresses, and identifies associated geocoded locations (i.e. latitude / longitude);
- The location server then uses the geocoded locations associated with visible MAC address to triangulate the approximate location of the user;
- and this approximate location is geocoded and sent back to the user's device.

How do your cars collect this WiFi data?
Visibly attached to the top of the car is a commercially available radio antenna. This antennae receives publicly broadcast WiFi radio signals within range of the vehicle. The equipment within the car operates passively, receiving signals broadcast to it but not actively seeking or initiating a communication with the access point.

Why didn't you let the German DPA see the car?
We offered to let them examine it last year --it is totally untrue to say we would not let them see the car. They are still welcome to do so.

How do you collect 3-D building imagery?
We collect 3D geometry data with low power lasers (similar to those used in retail scanners).

Is this safe?
Yes.

You can also read the WiFi submission we made today to several national data protection authorities.

Posted by Peter Fleischer, Global Privacy Counsel

** Added additional sentence to first bullet point.

Russia (1)
Single Market (4)
SMEs (2)
Street View (4)
Switzerland (1)
Telecoms (4)
The Netherlands (1)
United Kingdom (2)
YouTube (4)

Google Street View snooped WiFi for personal data

Network payloads collected 'by mistake'

By **Cade Metz and Dan Goodin in San Francisco** • **Get more from this author**

Posted in Security, 14th May 2010 22:52 GMT

Google has said that its world-roving Street View cars have been collecting information sent over open WiFi networks, contradicting previous assurances by the company.

This means that Google may have collected emails and other private information if they traveled over WiFi networks while one of the cars was in range. Previously, the company said no payload data was ever intercepted.

In a blog post published on Friday afternoon, the company said that it collected the data by "mistake" and that the data has not been used in any Google products. Street View cars have now been grounded, according to the post, and the company has promised to delete the data. But before doing so, it will be asking regulators in "the relevant countries" how this should be done.

Google declined to comment on the matter, instead pointing us back to its blog post. It arrives less than three weeks after the company said that such data was not being collected. But since then, Google conducted a review of the data being collected by its Street View cars after the data protection authority (DPA) in Hamburg, Germany requested such an audit.

Ginger McCall, a staff counsel with the Electronic Privacy Information Center (EPIC), a public watchdog, calls the data collection a "violation of customers' trust," and she questions Google's claim that it was collecting the data by mistake. "People need to ask why was Google was collecting this information," McCall told *The Reg*. "It's difficult to believe that this would be done accidentally.

"This really flies in the face of their assertion that customers should just trust them."

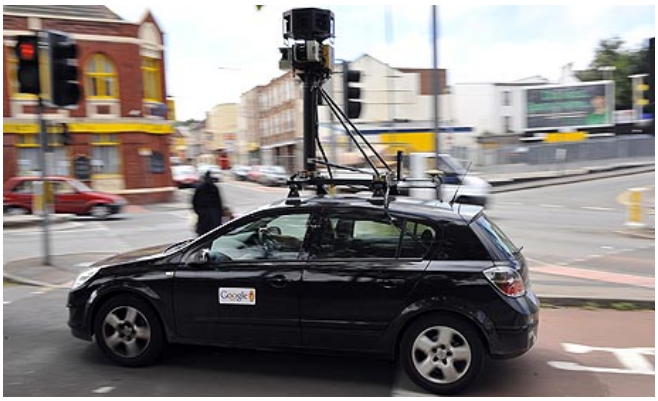
On April 27, in response to a complaint from the German DPA, a Google blog post said that in scanning open WiFi networks its Street View cars were collecting only the SSIDs that identify the networks and MAC addresses that identify particular network hardware, including routers. Google uses this data in products that rely on location data, such as Google Maps.

guardian.co.uk

Google admits collecting Wi-Fi data through Street View cars

German request for data audit reveals the web giant 'accidentally' stored payload information from open networks

Jemima Kiss
The Guardian, Saturday 15 May 2010



A Google mapping car with which the web giant admits accidentally collecting wifi data. Photograph: Ben Birchall/PA

Google has been accidentally gathering extracts of personal web activity from domestic wifi networks through the Street View cars it has used since 2007, it said last night.

It was discovered as a result of a data audit demanded by Germany's data protection authority, and is likely to inflame critics of Google concerned about the web giant's use of private data.

As well as systematically photographing streets and gathering 3D images of cities and towns around the world, Google's Street View cars are fitted with antennas that scan local wifi networks and use the data for its location services.

In a post on its European Public Policy blog on 27 April, Google stated that although it does gather wifi network names (SSIDs) and identifiers (Mac addresses) for devices like network routers, it does not gather "payload" data passed through those wifi networks.

But yesterday Google blogged that the audit had prompted it to "re-examine everything we have been collecting" and admitted its mistake.

"It is now clear that we have been mistakenly collecting samples of payload data from open wifi networks, even though we never used that data in any Google products."

Google said it amounted to 600GB, equivalent to a consumer hard drive, but that this data consisted only of fragments of activity from open wifi networks. Password-protected web services, such as banking or secure HTTP addresses, would not have been included, and neither would data from password-protected wireless networks.

Google blamed the mistake on a piece of legacy code from an experimental project that had been re-used to programme equipment on the Street View cars, and said it will ask a third party to oversee deletion of the data and its procedures.

"As soon as we became aware of this problem, we grounded our Street View cars and segregated the data on our network, which we then disconnected to make it inaccessible. We want to delete this data as soon as possible, and are currently reaching out to regulators in the relevant countries about how to quickly dispose of it."

Google said the discovery highlighted the vulnerability of data in open wifi networks. It has previously said other companies, including Skyhook and Microsoft, already scan wifi networks and gather information in this way.

The Google Street View feature in Google Maps, introduced in 2007, now displays street-level images from cities in nine countries, including 21 in the UK.

But it has faced regular concerns about privacy, which started in Britain on the day of the launch after users found images of a man throwing up in the street and another leaving a sex shop. In April last year, residents in Broughton barricaded roads to stop the Street View car entering the village, saying it would encourage crime and was an invasion of privacy.

Google is struggling with stricter privacy laws in Germany, where it has yet to launch the service, and Switzerland where it was introduced in August. Despite a flood of demands from the European Union, including wiping its Street View images after six months instead of 12, Google has said it remains committed to Street View in Europe. It said reports that it would stop mapping streets in any more EU countries are inaccurate.

Review: SmartDeploy Eases Windows 7 Migration

- Review: SharePoint 2010 Offers More
- Review: Ubuntu 10.04 LTS Server Hits Close To The Mark

More Products >>

Comment

Why Office 2010 Needs Both Mobility And The Cloud

- Palm Purchase Could Propel HP Into UC
- Green IT: An Unstable Coalition?
- Who Named The Orange / T-Mobile Merger?

More Comment >>
Print This Post Email This Post

Google Admits To Street View Data Gaff

Google says it will no longer collect WiFi data after finding its Street View cars have been collecting personal information for the last three years

- By:
  Clint Boulton
- May 17, 2010

Tags:Data, Google, privacy, Street View

Google on 14 May said it will no longer collect WiFi data after discovering that its Street View cars unwittingly collected personal information from citizens' networks, a violation of privacy sure to infl ame leaders of countries already wary of Google's data collection practices.

Google sends cars to patrol and take pictures of streets in countries all over the world for the Street View component of Google Maps.

The search engine initially said in April that its Street View Cars did not collect data that people share between WiFi networks and computers, although the cars did collect WiFi network names and router addresses. Google learned after conducting a data audit on behalf of the German government that this was incorrect.

Mistakenly Collecting Samples

"It's now clear that we have been mistakenly collecting samples of payload data from open (i.e. non-password-protected) WiFi networks, even though we never used that data in any Google products," wrote Alan Eustace, senior vice president of engineering and research.

Payload data can include user e-mails, passwords and Web browsing activity, data the sanctity of which Internet companies such as Google, Yahoo and Microsoft swear to protect. Germany, the United States, Britain and France were among the countries where Google collected this data.

The mistake was one of human engineering. Eustace said a Google programmer wrote a program that "sampled all categories of publicly broadcast WiFi data" and this code has accidentally been used since 2007 as part of the project of collecting "basic WiFi network data."

Eustace said Google "grounded our Street View cars and segregated the data on our network" when it became aware of the issue and is working hard to delete this data.

Moreover, Google's Street View cars will no longer collect WiFi network data and the company will begin offering an encrypted version of Google Search. Google began offering encrypted Gmail earlier in 2010 after Gmail accounts were accessed in a cyber-attack originating from China.

"The engineering team at Google works hard to earn your trust—and we are acutely aware that we failed badly here," Eustace wrote. "We are profoundly sorry for this error and are determined to learn all the lessons we can from our mistake."

Major Policy Blunder?

While Google's admission and apology seem forthright and humble, Eustace also sought to play down Google's data collection, a move that may undermine the admission of a major privacy blunder.

Eustace said the Street View cars "will typically have collected only fragments of payload data because our cars are on the move; someone would need to be using the network as a car passed by; and our in-car WiFi equipment automatically changes channels roughly five times a second."

He also said Google will review its procedures to "address these kinds of problems in the future."

However, future problems coming on the heels of this Street View fiasco, which follows the Google Buzz privacy debacle that exposed users' contacts online, could be disastrous for the company.

The Street View problem may be the killing shot government regulators require to advance a case that Google has violated consumer rights. Regulators could argue that given how much data Google collects, the Street View gaffe is proof that it lacks the necessary safeguards to preserve user privacy. Regulators could then sanction Google, imposing controls over how much data the company collects and how it is used.

Regulators in Europe were angry with Google, according to the New York Times.

Ilse Aigner, the German federal minister for food, agriculture and consumer protection, told the Times "it appears that Google has illegally tapped into private networks in violation of German law."

Privacy watchdogs such as Consumer Watchdog's John Simpson did not miss the opportunity.

"Once again Google has demonstrated a lack of concern for privacy," Simpson said 14 May in a statement sent to eWEEK. "Its computer engineers run amok, push the envelope and gather whatever data they can until their fingers are caught in the cookie jar. Then a Google executive apologises, mouthing bafflegab about how privacy matters to the company."

Simpson called for the Justice Department or the Federal Communications Commission to examine the Google case in the United States, and argued that the government must regulate the data all Internet companies store.

Privacy leaders in several countries, including Germany, the United Kingdom, France, China and Switzerland, have objected to Google Street View in the past. The Swiss federal data protection commissioner sued Google in November 2009 to demand that all faces and car plates be blurred and that Google erase images of walled gardens and private streets.

The European Union in February called for Google to provide advance notice when its Street View vehicles are roving European streets to take pictures and asked that these images be deleted after six months.

Categories: News, Search Engines, Security

Be the first to post

RSS - Feed for these comments.

Add a comment

Name (mandatory) :

E-mail (mandatory) :

Your eMail address will not be published

Web site :

Your comment :

Post your comment

Rick Klingbeil
Attorney
rick@klingbeil-law.com

Rick Klingbeil, PC
520 SW Sixth Avenue
Suite 950
Portland, OR 97204
Telephone: 503.473.8565
Facsimile: 503.914.0484

Sara Wegner
Paralegal
saraw@klingbeil-law.com

May 14, 2010

VIA US MAIL and FACSIMILE
Google, Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043
650.253.0001

Re: Prospective Class Action
Demand for Data Preservation

Dear Sir/Madam:

I am currently investigating, and will likely represent a class of plaintiffs in a legal claim / class action against Google, Inc. as a result of data collection performed by Google, Inc. through its fleet of vehicles responsible for photographing streets throughout the United States. This includes, but is not limited to the collection of data comprising or relating to personal information that consumers send over wireless networks, such as samples of payload data from open (i.e. non-password-protected) WiFi networks, users' email content and passwords, internet and web surfing activity, and other personal and user data and information that may have been collected by or on behalf of Google.

I have enclosed as Exhibit "A", a Demand for Preservation of Electronically Stored Information that informs you of this potential claim, and your duties to preserve information and data that may be evidence in the prospective claim.

Please contact me if you have questions.

Sincerely,

Rick Klingbeil

enclosure

Exhibit "A"

Demand for Preservation of Electronically Stored Information

On behalf of a potential class of plaintiffs ("prospective class plaintiffs") in a manner I am currently investigating, I hereby request that you preserve all data, documents, tangible things, and electronically stored information potentially relevant to or comprising data collected by Google through its fleet of vehicles responsible for photographing streets throughout the United States. This includes, but is not limited to data comprising or relating to personal information that consumers send over wireless networks, such as samples of payload data from open (i.e. non-password-protected) WiFi networks, users' email content and passwords, internet and web surfing activity, and other personal and user data and information that may have been collected by or on behalf of Google (hereinafter "collected data"). The above activities are referred to herein as "Google data collection activities".

At this point, it is likely that prospective plaintiffs will file a legal claim or class action against all or some of the responsible parties, including Google, Inc. as a result of the Google data collection activities.

As used in this document, “you” and “your” refers to Google, Inc., its successors, parents, subsidiaries, divisions or affiliates, and their respective officers, directors, agents, attorneys, accountants, employees, partners or other persons occupying similar positions or performing similar functions.

Much of the information subject to disclosure or responsive to future discovery requests in the prospective claim is likely stored on your current and former computer systems, servers, and other media and devices (including personal digital assistants, voice-messaging systems, online repositories, "cloud" based systems, and cell phones). This document provides you with notice that portions of this information may be relevant to, and subject to discovery in potential claims arising from the Google data collection activities, and provides notice of your duty to preserve such evidence and information.

Electronically stored information (hereinafter “ESI”) should be afforded the broadest possible definition and includes (by way of example and not as an exclusive list) potentially relevant information electronically, magnetically or optically stored as:

- Digital communications (e.g., e-mail, voice mail, instant messaging, radio transmissions);
- Word processed documents (e.g., Word or WordPerfect documents and drafts);
- Spreadsheets and tables (e.g., Excel or Lotus 123 worksheets);
- Accounting Application Data (e.g., QuickBooks, Money, Peachtree data files);
- Image and Facsimile Files (e.g., .PDF, .TIFF, .JPG, .GIF images);
- Sound Recordings (e.g., .WAV and .MP3 files);
- Video and Animation (e.g., .AVI and .MOV files);
- Databases (e.g., Access, Oracle, SQL Server data, SAP);
- Contact and Relationship Management Data (e.g., Outlook, ACT!);
- Calendar and Diary Application Data (e.g., Outlook PST, Yahoo, blog tools);
- Online Access Data (e.g., Temporary Internet Files, History, Cookies);

- Presentations (e.g., PowerPoint, Corel Presentations)
- Network Access and Server Activity Logs;
- Project Management Application Data;
- Computer Aided Design/Drawing Files; and,
- Back Up and Archival Files (e.g., Zip, .GHO, tape backup, online backup).

ESI resides not only in areas of electronic, magnetic, and optical storage media reasonably accessible to you, but also in areas you may deem *not* reasonably accessible. You are requested to *preserve* potentially relevant evidence from *both* these sources of ESI, even if you do not anticipate *producing* such ESI in the potential claim or any claim arising from the events described herein.

The request that you preserve both accessible and inaccessible ESI is reasonable and necessary, and in accord with the rules of civil procedure. For good cause shown, a court may order production of the ESI, even if it finds that it is not reasonably accessible. Accordingly, even ESI that you deem reasonably inaccessible *must be preserved in the interim* so as not to deprive the prospective plaintiffs of their right to secure the evidence or the Court of its right to adjudicate the issue. If evidence or things that are subject to your duty to preserve are not preserved, we anticipate requesting the court enter the appropriate curative sanctions, including, for example, adverse inference instructions to the jury, monetary sanctions, or the judicial determination that certain facts or claims are established.

Preservation Requires Immediate Intervention

We request that you act immediately to preserve potentially relevant or discoverable ESI including, without limitation, information obtained or created at any time during which the Google data collection activities occurred, through the date of this demand (and continuing for any subsequently produced ESI) and concerning or relating to:

1. The collection, storage, use, and any other activities related to the data obtained through the Google data collection activities;

2. ESI you may use to support claims or defenses in any prospective claim for damages or legal action arising from these events;

3. All data collected as a result of the Google data collection activities.

Please note that adequate preservation of ESI requires more than simply refraining from efforts to destroy or dispose of such evidence. We therefore request that you also affirmatively intervene to prevent loss due to routine operations and employ proper techniques and protocols suited to protection of ESI. *Be advised that sources of ESI are altered and erased by continued use of your computers and other devices.*

Booting a drive, examining its contents or running any application will irretrievably alter the evidence it contains and may constitute unlawful spoliation of evidence. Consequently, alteration and erasure may result from your failure to act diligently and responsibly to prevent loss or corruption of ESI.

Nothing in this demand for preservation of ESI should be understood to diminish your

concurrent obligation to preserve documents, tangible things and other potentially relevant evidence that does not fall within the definition or scope of ESI.

Suspension of Routine Destruction

We request that you immediately initiate a litigation hold for potentially relevant ESI, documents and tangible things, and to act diligently and in good faith to secure and audit compliance with such litigation hold. We further request that you immediately identify and modify or suspend features of your information systems and devices that, in routine operation, operate to cause the loss of potentially relevant ESI. Examples of such features and operations include:

- Purging the contents of e-mail repositories by age, capacity or other criteria;
- Using data or media wiping, disposal, erasure or encryption utilities or devices;
- Overwriting, erasing, destroying or discarding back up media;
- Re-assigning, re-imaging or disposing of systems, servers, devices or media;
- Running antivirus or other programs effecting wholesale metadata alteration;
- Releasing or purging online storage repositories;
- Using metadata stripper utilities;
- Disabling server or IM logging; and,
- Executing drive or file defragmentation or compression programs.

Guard Against Deletion

Your employees, officers or others may seek to hide, destroy or alter ESI and act to prevent or guard against such actions. Especially where company machines have been used for Internet access or personal communications, users may seek to delete or destroy information they regard as personal, confidential or embarrassing and, in so doing, may also delete or destroy potentially relevant ESI. This concern is not one unique to you or your employees and officers. It's simply an event that occurs with such regularity in electronic discovery efforts that, as a matter of course, we request that any custodian of ESI and their counsel guard against its occurrence.

Preservation by Imaging

We request that you take affirmative steps to prevent anyone with access to your data, systems and archives from seeking to modify, destroy or hide electronic evidence on network or local hard drives (such as by deleting or overwriting files, using data shredding and overwriting applications, defragmentation, re-imaging or replacing drives, encryption, compression, steganography or the like). With respect to local hard drives, one way to protect existing data on local hard drives is by the creation and authentication of a forensically qualified image of all sectors of the drive. Such a forensically

qualified duplicate may also be called a bitstream image or clone of the drive. Be advised that a conventional back up of a hard drive is not a forensically qualified image because it only captures active, unlocked data files and fails to preserve forensically significant data that may exist in such areas as unallocated space, slack space and the swap file.

Once obtained, we request that each such forensically qualified image be labeled to identify the date of acquisition, the person or entity acquiring the image and the system and medium from which it was obtained. We further request that each such image be preserved without alteration.

Preservation in Native Form

Certain ESI, including but not limited to spreadsheets and databases, will be sought in the form or forms in which it is ordinarily maintained. Accordingly, we request that you preserve ESI in such native forms, and request that you avoid any method to preserve ESI that removes or degrades the ability to search your ESI by electronic means, or that make it difficult or burdensome to access or use the information efficiently in the prospective litigation.

We also request that you refrain from actions that shift ESI from reasonably accessible media and forms to less accessible media and forms if the effect of such actions is to make such ESI not reasonably accessible.

Metadata

We request that you anticipate the need to disclose and produce system and application metadata and act to preserve it. System metadata is information describing the history and characteristics of other ESI. This information is typically associated with tracking or managing an electronic file and often includes data reflecting a file's name, size, custodian, location and dates of creation and last modification or access. Application metadata is information automatically included or embedded in electronic files but which may not be apparent to a user, including deleted content, draft language, commentary, collaboration and distribution data and dates of creation and printing. Be advised that metadata may be overwritten or corrupted by careless handling or improper steps to preserve ESI. For electronic mail, metadata includes all header routing data and Base 64 encoded attachment data, in addition to the To, From, Subject, Received Date, CC and BCC fields.

Servers

With respect to servers like those used to manage electronic mail (e.g., Microsoft Exchange, Lotus Domino) or network storage (often called a user's "network share"), we request that the complete contents of each user's network share and e-mail account be preserved. There are several ways to preserve the contents of a server depending upon, e.g., its RAID configuration and whether it can be downed or must be online 24/7.

Home Systems, Laptops, Online Accounts and Other ESI Venues

Although we expect that you will act swiftly to preserve data on office workstations and servers, we also request that you determine if any home or portable systems may contain potentially relevant data. To the extent that officers, board members or employees have sent or received potentially relevant

e-mails or created or reviewed potentially relevant documents away from the office, we request that you preserve the contents of systems, devices and media used for these purposes (including not only potentially relevant data from portable and home computers, but also from portable thumb drives, CD-R disks and the user's PDA, smart phone, voice mailbox or other forms of ESI storage.). Similarly, if employees, officers or board members used online or browser-based email accounts or services (such as AOL, Gmail, Yahoo Mail or the like) to send or receive potentially relevant messages and attachments, we request that the contents of these account mailboxes (including Sent, Deleted and Archived Message folders) be preserved.

From: Sara Wegner <saraw@klingbeil-law.com>
Subject: **Fwd: Successful transmission to 16502530001. Re: Re: Notice to Preserve Data**
Date: May 14, 2010 4:26:23 PM PDT
To: Rick Klingbeil <rick@klingbeil-law.com>

Sara Wegner
Paralegal
saraw@klingbeil-law.com

Begin forwarded message:

From: send@mail.efax.com
Date: May 14, 2010 4:22:07 PM PDT
To: saraw@klingbeil-law.com
Subject: **Successful transmission to 16502530001. Re: Re: Notice to Preserve Data**

eFax® Easy faxing anywhere.™

Dear Rick Klingbeil,

Re: Re: Notice to Preserve Data

The 6 page fax you sent through eFax.com to 16502530001 was successfully transmitted at 2010-05-14 23:21:59 (GMT).

The length of transmission was 265 seconds.

The receiving machine's fax ID: 1-650-618-1499.

Best Regards,

If you need additional assistance, please visit our online help center at http://www.efax.com/help/. Thank you for using the eFax service.

eFax.com

Customer Service
Online Help: http://www.efax.com/help/
Tel: 323-817-3205 (US) or 0870 711 2211 (UK)
Email: help@mail.efax.com

Google

CERTIFICATE OF SERVICE

I, Rick Klingbeil, hereby certify that on May 18, 2010 I electronically filed the preceding document with the clerk of the court using the CM/ECF filing system.

Because no appearance has been made by defendant or its counsel, a true and correct copy of this document has also been served by hand delivery to defendant's registered agent within the state of Oregon, and mailed via first class mail to defendant at the following addresses:

Hand Delivery to:

Google, Inc.
c/o The Corporation Trust Company
388 State Street, Suite 420
Salem, OR 97301

First Class Mail to and Facsimile Transmission to:

Google Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043

Facsimile No.: 1-650-253-0001

DATED: May 18, 2010.

RICK KLINGBEIL, P.C.

Rick Klingbeil, OSB #933326
of Attorneys for Plaintiffs